IN THE CLAIMS

1. (currently amended) An information processing system for distributing encrypted message data, said system comprising:

a receiving device, including:

holding means for holding a key set that is specific to said receiving device and which includes a portion of a plurality of node keys and a corresponding leaf key, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of leaves, the portion of the plurality of node keys being the node keys associated with the nodes disposed along a particular path from the root node of the hierarchical tree structure to a particular one of the plurality of leaves that is associated with said receiving device and with its corresponding leaf key, and

encryption processing means for decrypting encrypted message data distributed to said receiving device by using the key set; and

a distributing device, including:

message data generating means for generating an enabling key block (EKB) using one or more keys selected from the group consisting of the portion of the plurality of node keys and the corresponding leaf key, and

message data distributing means for distributing a storage medium storing first message data that includes data in which first content is encrypted with a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the

enabling key block (EKB), and storing second message data that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB).

2. (previously presented) The information processing system according to claim 1, wherein said encryption processing means of said receiving device obtains a renewal node key by decrypting the enabling key block (EKB).

3. (cancelled)

4. (previously presented) The information processing system according to claim 1, wherein at least one of the first message data and the second message data includes an authentication key used in authentication processing.

5. (previously presented) The information processing system according to claim 1, wherein at least one of the first message data and the second message data includes a key for generating an integrity check value (ICV) of its content.

6. (previously presented) The information processing system according to claim 1, wherein at least one of the first message data and the second message data includes a program code.

7. (cancelled)

8. (previously presented) The information processing system according to claim 1, wherein said message data distributing means and said receiving device each include associated authentication processing means for executing authentication processing, and a distribution of said message data is performed on the condition that the authentication processing between said message data distributing means and said receiving device has been completed.

9. (previously presented) The information processing system according to claim 1, wherein an intermediate device is disposed between said message data distributing means and said receiving device, and said message data distributing means generates and distributes enabling key block (EKB) data and encrypted first and second message data that can be decrypted only in target devices targeted for distributing said message data.

10. (previously presented) The information processing system according to claim 1, wherein the hierarchical tree structure includes a category group that includes only the nodes and leaves which are subordinate to a further one of the plurality of nodes;

wherein the category group is associated with a set of devices that belong to a category defined by a kind of device, a kind of a service or a kind of a managing means.

11. (previously presented) The information processing system according to claim 10, wherein the category group further includes one or more sub-category groups in the hierarchical tree structure;

wherein the sub-category group is associated with a sub-set of devices that belong to a category defined by another kind of device, kind of a service, or kind of a managing means.

12. (currently amended) An information processing method for distributing encrypted message data, said method comprising:

generating a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of leaves, the plurality of leaves being

associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices;

generating an enabling key block (EKB) using one or more keys selected from the group consisting of the plurality of node keys and the plurality of leaf keys;

distributing a storage medium storing first message data that includes data in which first content is encrypted by a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), the content key encryption key being the renewal node key; and

decrypting, at a given one of the plurality of different devices, the encrypted first message data using an associated key set that is specific to and stored in that device and using the data in which the content key encryption key is encrypted by the enabling key block (EKB), the associated key set including a specific portion of the plurality of node keys that are associated with the nodes disposed along a particular path from the root node of the hierarchical tree structure to a particular one of the plurality of leaves that is associated with that device and including the leaf key associated with that device so

that the key set associated with a given one of the plurality of devices is different than the key set associated with another one of the plurality of devices.

13. (previously presented) The information processing method according to claim 12, wherein said decrypting step includes a renewal node key obtaining step of obtaining a renewal node key by decrypting the enabling key block (EKB), and a message data decrypting step for executing decryption of the encrypted first message data using the renewal node key.

14. (cancelled)

15. (previously presented) The information processing method according to claim 12, wherein at least one of the first message data and the second message data includes an authentication key used in the authentication processing.

16. (previously presented) The information processing method according to claim 12, wherein at least one of the first message data and the second message data includes a key for generating an integrity check value (ICV) of its content.

17. (previously presented) The information processing method according to claim 12, wherein at least one of the first message data and the second message data includes a program code.

18. (cancelled)

19. (previously presented) The information processing method according to claim 12, further comprising an authentication processing step for executing authentication processing, and

wherein said message data distributing step is performed on the condition that said authentication processing step has been completed.

20. (previously presented) The information processing method according to claim 12, wherein said message data distributing step generates and distributes enabling key block

(EKB) data and encrypted first and second message data that can be decrypted only in a target device targeted for receiving said message data.

21. (currently amended) An information recording medium having stored therein data, said data comprising:

a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of leaves, the plurality of leaves being associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices;

an enabling key block (EKB) which is encrypted using one or more keys selected from the group consisting of the plurality of node keys and the plurality of leaf keys;

first message data that includes data in which first content is encrypted with a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on said information recording medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB); and

second message data that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on said information recording medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB).

22. (cancelled)

23. (cancelled)

24. (previously presented) The information recording medium according to claim 21 wherein said information recording medium stores an integrity check value (ICV) of at least one of the first content and the second content.

25. (currently amended) A computer-readable medium for storing instructions for carrying out a method of decrypting encrypted content, said method comprising:

obtaining a storage medium storing first message data that includes data in which first content is encrypted by a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB);

obtaining an enabling key block (EKB) using at least one or more keys selected from the group consisting of a plurality of node keys and a plurality of leaf keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of a plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of leaf keys being associated with a plurality of leaves whereby a given one of the plurality of leaf keys is associated with a specific one of the plurality of leaves, the plurality of nodes being arranged according to a hierarchical tree structure having a root

node and the plurality of leaves, at least one of the plurality of node keys being renewable using the renewal node key;

decrypting, using the enabling key block, the data in which the content key encryption key is encrypted;

decrypting, using the content key encryption key, the data in which content key is encrypted; and decrypting the at least one of the encrypted first content using the content key.

26. (currently amended) An information processing method for distributing encrypted message data, said method comprising:

generating a plurality of node keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of the plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and a plurality of leaves, the plurality of leaves being associated with a plurality of leaf keys and with a plurality of devices whereby a given one of the plurality of leaves is associated with a specific one of the plurality of leaf keys and with a particular one of the plurality of devices;

generating an enabling key block (EKB) using one or more keys selected from the group consisting of the plurality of node keys and the plurality of leaf keys; and

generating a storage medium storing first message data that includes data in which first content is encrypted by a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data

that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), to distribute the first message data and the second message data to a plurality of devices.

27. (cancelled)

28. (previously presented) The information processing method according to claim 26, wherein at least one of the first message data and the second message data includes an authentication key used in authentication processing.

29. (previously presented) The information processing method according to claim 26, wherein at least one of the first message data and the second message data includes a key for generating an integrity check value (ICV) of contents.

30. (cancelled)

31. (currently amended) An information processing method, comprising:

obtaining a storage medium storing first message data that includes data in which first content is encrypted by a first content key, data in which the first content key is encrypted by a content key encryption key, and a link to a location on the storage medium wherein data is stored in which the content key encryption key is encrypted by the enabling key block (EKB), and storing second message data that includes data in which second content is encrypted by a second content key, data in which the second content key is encrypted by the content key encryption key, and another link to the location on the storage medium wherein the data is stored in which the content key encryption key is encrypted by the enabling key block (EKB);

obtaining the enabling key block (EKB) using at least one or more keys selected from the group consisting of a plurality of node keys and a plurality of leaf keys, the plurality of node keys being associated with a plurality of nodes whereby a given one of a plurality of node keys is associated with a particular one of the plurality of nodes, the plurality of leaf keys being associated with a plurality of leaves whereby a given one of the plurality of leaf keys is associated with a specific one of the plurality of leaves, the plurality of nodes being arranged according to a hierarchical tree structure having a root node and the plurality of leaves, at least one of the plurality of node keys being renewable using the renewal node key;

decrypting, using the enabling key block (EKB), the data in which the content key encryption key is encrypted;

decrypting, using the content key encryption key, the data in which content key is encrypted; and decrypting the encrypted first content using the content key.

32. - 33. (cancelled)

34. (new) The information processing system according to claim 1, wherein a same encryption key is used for both the first content key and the second content key.

35. (new) The information processing method according to claim 12, wherein a same encryption key is used for both the first content key and the second content key.

36. (new) The information recording medium according to claim 21, wherein a same encryption key is used for both the first content key and the second content key.

37. (new) The computer-readable medium according to claim 25, wherein a same encryption key is used for both the first content key and the second content key.

38. (new) The information processing method according to claim 26, wherein a same encryption key is used for both the first content key and the second content key.

39. (new) The information processing method according to claim 31, wherein a same encryption key is used for both the first content key and the second content key.